



DEPARTMENT OF THE NAVY  
OFFICE OF THE SECRETARY  
1000 NAVY PENTAGON  
WASHINGTON, D.C. 20350-1000

SECNAVINST 3300.2C  
DUSN  
13 AUG 2018

SECNAV INSTRUCTION 3300.2C

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY ANTITERRORISM PROGRAM

Ref: See enclosure (1)

Encl: (1) References  
(2) Responsibilities  
(3) Acronyms and Definitions

1. Purpose. To implement the guidance set forth in references (a) through (e) by:

a. Establishing Department of the Navy (DON) Antiterrorism (AT) Program policies and procedures;

b. Assigning responsibilities;

c. Providing guidance and information to reduce the vulnerability of DON military and civilian personnel, family members, contractors, resources, facilities, and ships to terrorist acts;

d. This constitutes a major revision and should be reviewed in its entirety.

2. Cancellation. SECNAVINST 3300.2B.

3. Definitions. See enclosure (3).

4. Applicability

a. This instruction applies to the Office of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all U.S. Navy and U.S. Marine Corps installations, commands, activities, field offices, and all other organizational entities within the DON. Additionally, this instruction applies to all personnel, to include military Service Members and their dependents, DON civilian work force, DON contractors, and applicable family

members of DON personnel. It complements existing Department of Defense (DoD) and DON physical security directives. AT responsibilities for defense contractors are contained in reference (a). AT responsibilities for DON elements and personnel under security responsibility of the Department of State (DOS) are also contained in references (a) and (d).

b. This instruction does not apply to DON elements and personnel under the security responsibility of DOS pursuant to Sections 4801, 4802, and 4805 of Title 22, U.S.C.; the December 16, 1997, Memorandum of Understanding between the DOS and DoD; and DoDI 5210.84, including those assigned to international organizations, such as the Multinational Force and Observers. These DON elements and personnel must comply with National Security Council Overseas Security Policy Board and DOS security standards instead of the standards prescribed in reference (a) and this instruction.

## 5. Policy

a. Commanders should give special emphasis to reducing the vulnerability of personnel, family members, resources, facilities, and critical infrastructure under DON cognizance to terrorist acts. The DON AT program should be an "all-encompassing program" using a system to promote efficiencies and sustainability.

b. Force Protection (FP) is the Commander's responsibility. Commanders must balance AT considerations with mission accomplishment imperatives utilizing operational risk management.

c. All Service Members, DON civilians, and DON family members, as applicable, will follow the Geographic Combatant Commander's AT policies and shall comply with theater, country, and special clearance requirements as specified in references (b) and (d).

d. DON personnel who are permanently or temporarily assigned to installations, including non-DON tenants, of the command's AT program, will adhere to the Region/Installation Commander's guidance pertaining to the local terrorist threat, personal protective, and travel security measures that can reduce personal vulnerability.

e. Commanders will liaise with Federal, State, Local, tribal, and Foreign Agencies in accordance with approved Mutual

Aid Agreements, Memoranda of Understanding (MOUs), Memoranda of Agreement (MOAs), and local agreements. Commanders will ensure AT plans and event management is communicated to and with all concerned parties.

6. Responsibilities. See enclosure (2).

7. Unmanned Aircraft Systems (UAS)

a. Guidance for the domestic use of UAS is provided in references (f) and (g).

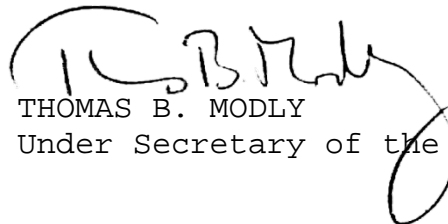
b. Guidance for the countering of unmanned aircraft (C-UA) is provided in references (h), (i), and (j).

8. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page:

<https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx>.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

  
THOMAS B. MODLY  
Under Secretary of the Navy

Distribution:

Electronic only, via Department of the Navy Issuances website  
<http://doni.documentservices.dla.mil>.

**REFERENCES**

- (a) DoD Instruction 2000.12 of 1 March 2012
- (b) DoD Directive 4500.54E of 12 December 2009
- (c) DoD Directive 5100.03 of 9 February 2011
- (d) DoD Instruction O-2000.16, Volume 1 of 17 November 2016
- (e) DoD Instruction O-2000.16, Volume 2 of 17 November 2016
- (f) DEPSECDEF Memo 15-002, Guidance for the Domestic Use of Unmanned Aircraft Systems of 17 February 2015
- (g) COMNAVAIRFORINST 3710.9 Unmanned Aircraft Systems of November 2017
- (h) DEPSECDEF Memo 17-00X, Supplemental Guidance for Countering Unmanned Aircraft of 5 July 2017 (NOTAL)
- (i) DEPSECDEF Memo 16-003, Interim Guidance for Countering Unmanned Aircraft of 18 August 2016 (NOTAL)
- (j) Counter Unmanned Aircraft System Guidance and Considerations, issued by Commander U.S. Fleet Forces Command, dated February 5, 2018 (NOTAL)
- (k) 10 U.S.C. §5013
- (l) SECNAVINST 5500.36
- (m) Unified Facilities Criteria 4-010-01, DoD Minimum Antiterrorism Standards for Buildings of 1 October 2013
- (n) Unified Facilities Criteria 4-020-01, DoD Security Engineering Facilities Planning Manual of 11 September 2008
- (o) DoD Instruction 2000.12 of 8 May 2017

13 AUG 2018

## **RESPONSIBILITIES**

1. The Under Secretary of the Navy (UNSECNAV), is designated as the deputy and principal assistant to the SECNAV, and acts with the full authority of SECNAV in managing the DON, per reference (k).

2. The Deputy Under Secretary of the Navy (DUSN) is the DON Security Executive and leads the DON Security Enterprise, per reference (l).

3. The DUSN Senior Director for Security shall:

a. Develop DON AT policy guidance and provide oversight of DON AT efforts.

b. Serve as the principal advisor to the DUSN on all AT matters.

4. The Director of the Navy Criminal Investigative Service (DIRNCIS) will:

a. Provide prompt dissemination of information on terrorist threats, including specific warning of threats against DoD elements and personnel.

b. Conduct liaison with Federal, State, and local agencies and foreign agencies for the collection and exchange of international terrorist threat information. NCIS is the primary liaison to civil Law Enforcement authorities but this relationship does not preclude local Security Officers, Antiterrorism Officers(ATO), and Provost Marshals from coordinating with local Law Enforcement when necessary and applicable.

c. Establish and implement Counterintelligence (CI) initiatives to identify and counter espionage, international terrorism, and the CI insider threat.

5. The CNO and the CMC, as appropriate, shall implement the provisions of reference (a), including:

a. Develop AT programs for the Department, to include reserve components, and support them with adequate resources for manpower, planning, and funding. Ensure that existing physical security, base defense, fire, safety, medical, emergency management, and law enforcement programs address terrorism as a potential threat to DON elements and personnel.

b. Support the geographic and functional Combatant Commanders and ensure that resources are adequately programmed in the DON budgets to implement their AT programs per reference (c). Coordinate with the geographic and functional Combatant Commanders to ensure adequate protection of forces, installations, and DON personnel and dependents.

c. Incorporate AT into DON doctrine, ensuring the doctrine is compatible with both DoD and joint doctrine.

d. Institute AT Level I training programs per references (a) and (d). Additionally, ensure the appointment of a trained AT Level II professional to administer the program. The position may be designated as a "Special Staff Officer" working directly for the Region, Installation, Brigade or Battalion Commander or respective N/S/G-3.

e. Identify and designate high-risk billets. Provide AT training to those personnel assigned to high-risk billets, their family members, and others, as applicable.

f. Ensure that military Service Members and their dependents, DON civilian work force, DON contractors, and applicable family members of DON personnel comply with reference (d), and those scheduled for permanent change of station to foreign countries receive the required AT training.

g. In coordination with Geographic Combatant Commanders, ensure prompt dissemination of information on terrorist threats, including specific warning of threats against DoD elements and personnel.

h. In coordination with the Chairman, Joint Chiefs of Staff, and Commanders of Combatant Commands, address AT considerations in recommending tour lengths and determine whether restrictions should be placed on accompanying family members for personnel assigned to overseas activities.

i. Establish military construction programming policies per existing reference (g) to ensure AT protective features for facilities and installations are included in the planning, design, budgeting, and execution of military and minor construction projects to physical security requirements for military construction projects must be determined during the planning process. Applicable physical security and risk-and threat-appropriate physical security capabilities will be developed as requirements and incorporated into designs.

13 AUG 2018

Their incorporation will be monitored during construction to ensure appropriate capabilities are present in completed facilities. This includes implementing procedures to:

(1) Prioritize requirements using the Joint Staff Capabilities Integration and Development System (JCIDS).

(2) Embrace the use of existing commercial-off-the-shelf and Government-off-the-shelf (GOTS) systems AT products.

(3) Expedite the transition of emerging AT technologies.

(4) Comply with the Combatting Terrorism Readiness Initiative Fund (CbT-RIF), Combatant Commander Initiative Fund (CCIF) requirements, and Program Objective Memoranda (POM) submission process.

(5) Leverage the Naval Facilities Engineering Command Physical Security Technology Division (CI8) and coordinate with Systems Commands and Office of Naval Research (ONR) research, development, testing, and evaluation (RDT&E) activities.

(6) Establish military construction programming policies per existing references (m) and (n) to ensure AT protective features for facilities and installations are included in the planning, design, budgeting, and execution of military and minor construction projects.

(7) Ensure that DON installations, units, exercises, ports, ships, residences, facilities, or other sites and activities are assessed per reference (d). Ensure installations develop, maintain, and implement AT plans and programs that incorporate measures in concert with DON, Combatant Commanders, and DoD standards and correct or mitigate vulnerabilities identified in assessments.

(8) Identify the resources programmed to implement and correct identified vulnerabilities and maintain the AT program for DON components as part of the Planning, Programming, Budgeting, and Execution (PPBE) process.

(a) Ensure life-cycle costs are programmed and funded for CbT-RIF and CCIF projects.

(b) Update and maintain the Core Vulnerability Assessment Management Program (CVAMP) and the Navy Mission

Assurance Risk Management System (N-MARMS). Ensure all AT vulnerability assessment data, be it a self-assessment, higher headquarters assessment, Joint Mission Assurance Assessment, and/or actions planned to mitigate them are entered into CVAMP or N-MARMS respectively.

(c) Update and maintain the Defense Readiness Reporting System-Navy (DRRS-N). Ensure all FP vulnerabilities and actions planned to mitigate them are entered into DRRS-N.

(9) Ensure that the DON, utilizing NCIS competency, has the capability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack through the implementation of eGUARDIAN, DoD Law Enforcement Defense Data Exchange (D-DEX), CI, Criminal Intelligence, Multiple Threat Alert Center (MTAC), Hostage/Crisis Negotiation Teams, and Counterterrorism (CT) databases and skillsets.



## ACRONYMS AND DEFINITIONS

### Acronyms:

AT	Antiterrorism
ATO	Antiterrorism Officer
CbT-RIF	Combatting Terrorism Readiness Initiative Fund
CCIF	Combatant Commander Initiative Fund
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
COCOM	Combatant Commander
CONUS	Continental United States
CT	Counterterrorism
C-UA	Countering Unmanned Aircraft
C-VAMP	Core Vulnerability Assessment Management Program
D-DEX	DoD Law Enforcement Defense Data Exchange
DIRNCIS	Director of the Naval Criminal Investigative Service
DRRS-N	Defense Readiness Reporting System-Navy
DUSN	Deputy Under Secretary of the Navy
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DON	Department of the Navy
DOS	Department of State
FP	Force Protection
GOTS	Government Off the Shelf
JCIDS	Joint Staff Capabilities Integration and Development System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTAC	Multiple Threat Alert Center
NCIS	Navy Criminal Investigative Service
NLW	Non-Lethal Weapon
N-MARMS	Navy Mission Assurance Risk Management System
ONR	Office of Naval Research
PPBE	Planning, Programming, Budgeting, and Execution
POM	Program Objective Memoranda
RDT&E	Research, Development, Testing, and Evaluation
SECNAV	Secretary of the Navy
SYSCOM	Systems Command
UAS	Unmanned Aircraft Systems
UNSECNAV	Under Secretary of the Navy
U.S.C.	United States Code
VCNO	Vice Chief of Naval Operations

13 AUG 2018

Definitions: Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

1. ATO. The principal military or civilian advisor charged with managing the AT program for the commander or DoD civilian exercising equivalent authority (reference (d)).

2. AT program. AT is not only a sub-element of combating terrorism, but also a subset of the broader FP construct. The AT program is a component of Mission Assurance.

a. The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel and their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents.

b. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program.

c. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource application, and a program review (reference (d)).

3. AT Risk Management. The process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. AT risk management is one of the five minimum elements of an AT program. The end products of the AT program risk management process shall be the identification of DoD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (threat assessment, criticality assessment, and vulnerability assessment), the commander or DoD civilian manager or director must determine which DoD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate, or prepare for a terrorist incident (reference (o)).

13 AUG 2018

4. Commander. A person assigned to a command position in a military organization, including military directors of Defense Agencies and DoD Field Activities. Refers to personnel assigned to command positions at all levels and their civilian equivalents (reference (d)).

5. DoD Personnel. Uniformed Military Service Members and DoD Federal civilian employees hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment (reference (d)).

6. Imminent. As used in this policy, "imminent" has a broader meaning than "immediate" or "instantaneous." The concept of "imminent" should be understood to be elastic, that is, involving a period of time dependent on the circumstances, rather than the fixed point of time implicit in the concept of "immediate" or "instantaneous." Thus, a subject may pose an imminent danger even if he or she is not at that very moment pointing a weapon at the officer if, for example, he or she has a weapon within reach or is running for cover carrying a weapon or running to a place where the officer has reason to believe a weapon is available.

7. MOA. A type of intra-agency or interagency agreement between two or more parties, which includes specific terms that are agreed to, and a commitment by at least one party to engage in action. It includes either a commitment of resources or binds a party to a specific action (reference (d)).

8. Terrorism Consequence Management. DoD preparedness and response for mitigating the consequences of a terrorist incident, including the terrorist use of Weapons of Mass Destruction. DoD consequence management activities are designed to support a lead Federal agency and include measures to alleviate damage, loss of life, hardship, or suffering caused by the incident; protect public health and safety; and restore emergency essential government services (reference (d)).

9. Terrorism Incident Response Measures. A set of procedures established for response forces to deal with the effects of a terrorist incident (reference (d)).

10. Vulnerability. With respect to the DoD AT program, a situation or circumstance which, if left unchanged, may result in the loss of life or damage to mission-essential resources from a terrorist attack. It includes the characteristics of an

13 AUG 2018

installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a terrorist attack (reference (d)).

11. Vulnerability Assessment. A DoD, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a terrorist attack.